

DATABASE SECURITY

**The more you sweat in training, the less you'll
bleed in battle.**

OUTLINE

- Why is database security important?
- Our environment
- General Strategies and Tactics for Hardening Databases
- Oracle
- SQL Server
- MySQL



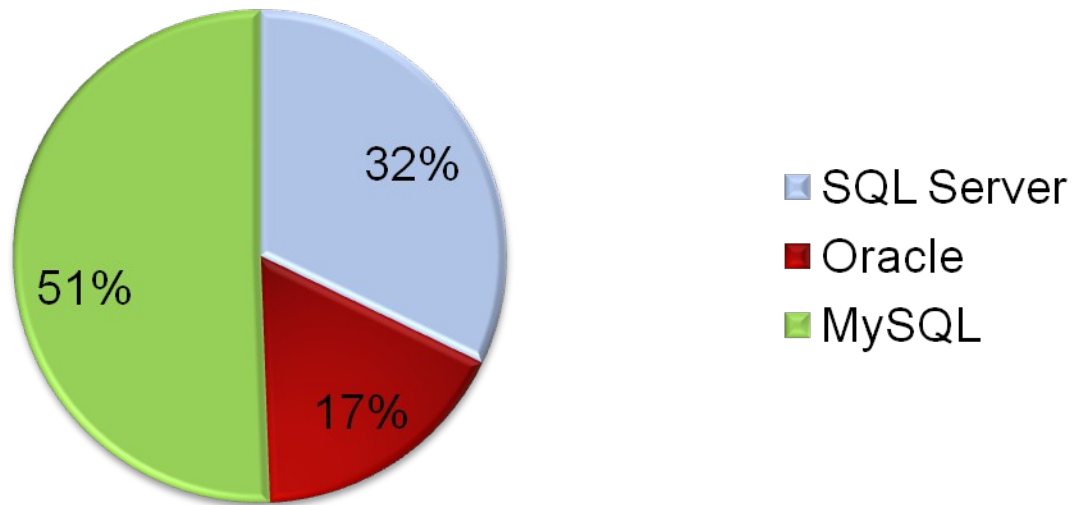
WHY IS DATABASE SECURITY IMPORTANT?

- Databases often store data which is sensitive in nature
- Incorrect data or loss of data could negatively affect business operations
- Databases can be used as bases to attack other systems from



OUR ENVIRONMENT

Database Services*



*Figures found by scanning for open ports commonly used by the respective software.



HARDENING DATABASES – GENERAL STRATEGIES AND TACTICS

- Principle of Least Privilege!
- Stay up-to-date on patches
- Remove/disable unneeded default accounts
- Firewalling/Access Control
- Running Database processes under dedicated non-privileged account.
- Password Security
- Disable unneeded components
- Stored Procedures and Triggers



PRINCIPLE OF LEAST PRIVILEGE

- If X service doesn't need access to all tables in Y database... then don't give it access to all tables.
 - Example: A web application that reads a list of people from a database and lists them on a website. The database also contains sensitive information about those people. The account used by the web application should not be allowed to read the table that contains sensitive non-public information.
- Do not give accounts privileges that aren't needed
 - Unneeded privileges to accounts allow more opportunity for privilege escalation attacks.



HARDENING DATABASES – FIREWALL/ACCESS CONTROL

- Throttling connections – make it harder for the bad guys to brute-force or guess passwords
 - Use firewall software like IPTables
 - Xinetd may be useful for throttling
 - It's possible that throttling could deny access to applications which make a large amount of connections legitimately.
- Reducing the surface area of attack with firewall rules
 - Don't let the world connect to your database server.



HARDENING DATABASES – PASSWORD SECURITY

- Strong passwords are a must
 - Constant brute-force attacks are happening across campus. Esp. against SQL Server
- Default passwords are a problem
- MySQL: root@localhost:<blank>
- SQL Server: sa:<blank> (Old, but still seen sometimes)
- Oracle: ...
- Built in password policy control seems rare
 - How can we enforce password policy?



HARDENING DATABASES – STORED PROCEDURES, TRIGGERS

- Stored Procedures and Triggers can lead to privilege escalation and compromise. Be sure to be thinking about security implications when allowing the creation of, and creating these.



HARDENING DATABASES – DISABLE UNNEEDED COMPONENTS

- Just like disabling unneeded services for an operating system is a good idea disabling unneeded components for databases is a good idea.
 - XML FTP (Oracle)
 - Named Pipes access (SQL Server)



SELECT slides FROM
presentation. **Oracle**



ORACLE'S VULNERABILITY HISTORY

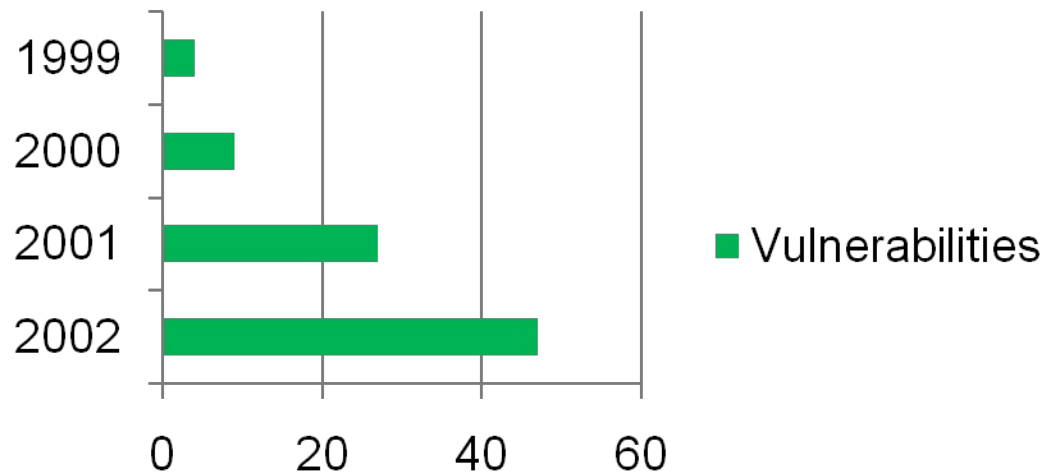
If [the] Oracle could see into the future... the “Unbreakable” marketing campaign may have not been a good idea.

- A search on milw0rm's exploit catalogue returns
 - 27 exploits dated from 11/16/2000 – 07/19/2007



VULNERABILITY HISTORY (CONT.)

Data and quote from *The Oracle Hacker's Handbook*:



“[...] 2003 and beyond [...] the numbers went through the roof [...]”



HARDING ORACLE - TNS LISTENER

TNS Listener

- “The TNS Listener is the hub of all communications in Oracle. [...] When a client wishes to access the database server, the client connects first to the Listener. [...] **In versions of Oracle prior to 10g, the TNS Listener could be administered remotely. What makes this particularly dangerous is the fact that by default the Listener is installed without a password [...]**”

– *The Database Hacker's Handbook*



HARDING ORACLE - TNS LISTENER

- Set a password for TNS Listener Administration
 - listener.ora file
 - PASSWORDS_listenername = somepass
 - Use the lsnrctl utility
 - LSNRCTL> change_password



HARDENING ORACLE - DEFAULT ACCOUNTS

- Decent amount of default accounts
 - Be aware what they are
 - Ensure the passwords do in fact get changed appropriately
- 10g forces admin to set passwords for many default accounts on install and may lock or expire them.



SELECT slides FROM

presentation. **SQL Server**



HARDENING SQL SERVER – LOCAL ADMINS

- Removing Local Builtin\Administrators group from sysadmins
 - If they are an administrator on a system running SQL Server they can get to anything in any database.



HARDENING SQL SERVER - AUTHENTICATION

- If configured to use Windows Authentication password policy can be enforced!



HARDENING SQL SERVER – XP_CMDSHELL

- Do not enable this on install of SQL Server 2k5 unless absolutely necessary



SELECT slides FROM
presentation.**MySQL**



HARDING MYSQL – DISABLING NETWORK ACCESS

- If your Database is only for being accessed by someone/something on the same machine
 - disable network-based access with the `--skip-networking` option
 - Firewall off the port MySQL is listening on (typically port 3306)



HARDENING MYSQL - ACCOUNT TYPES

- Identity is determined by username AND the location connected from - Coolness
- Scope Identities appropriately
 - Allow bob to login from any uiowa.edu hostname
 - GRANT [...] ON somedb.sometable TO BOB@'%.uiowa.edu';
 - Allow bob to login from any campus IP address
 - GRANT [...] ON somedb.sometable TO BOB@'128.255.0.0/255.255.0.0';



HARDENING MYSQL – ENCRYPTING TRAFFIC

- MySQL supports encrypting traffic with SSL
 - Consider using `GRANT ... REQUIRE SSL` or similar for an account
 - Useful for accounts that may be accessing sensitive data and/or data that is required to be encrypted by some requirement.

RESOURCES

- D.Litchfield, C.Anley, J. Heasman, B. Grindlay, ***The Database Hacker's Handbook – Defending Database Servers***, Indianapolis: Wiley Publishing Inc., 2005.
 - Available on Books 24x7
- D.Litchfield, ***The Oracle® Hacker's Handbook: Hacking and Defending Oracle***, Indianapolis: Wiley Publishing Inc., 2007.
 - Available on Books 24x7
- <http://databasesecurity.com>
- <http://blogs.msdn.com/raulga/archive/2007/01/04/dyna>
- <http://msdn.microsoft.com/msdnmag/issues/05/06/SQL>
- <http://www.cgisecurity.com>



Questions or Comments?

